ABSTRACT

A system architecture for thwarting denial of service attacks on a victim data center is described. The system includes a first plurality of data monitors that monitor network traffic flow through the network. The first plurality of monitors is disposed at a second plurality of points in the network. The system includes a central controller that receives data from the plurality of monitors, over a hardened, redundant network. The central controller analyzes network traffic statistics to identify malicious network traffic. In one embodiment, a gateway device is disposed to pass network packets between the network and the victim site. The gateway includes a computing device executing a process to build a histogram for any attribute or function of an attribute of network packets and a process to determine if the values of the attribute exceed normal, threshold values expected for the attribute to indicate an attack on the site.